

EXHIBIT 1

4. Due to the complexity of this action, which is estimated to involve millions of pages of documents, and to facilitate the flow of discovery material, at the time of initial production, the producing party may designate an entire document as “Confidential” if it believes in good faith that any part of the document is confidential or if the document falls within a category of documents that the designating party believes is likely to contain a large volume of Confidential material.

5. After review, the receiving party may request that the producing party identify for specific documents (no more than 500 documents in a 30 day period) what parts of those documents are confidential. The challenge process described below in paragraph 16 may then be used to resolve any disputes as to those designations. If it comes to the designating party’s attention that information or items that it designated for protection do not qualify for protection, that designating party must promptly notify all other Parties that it is withdrawing its mistaken designation.

6. To the extent that information stored or recorded in the form of electronic or magnetic media (including information, files, databases, or programs stored on any digital or analog machine-readable device, computers, Internet sites, discs, networks, or tapes) (“Computerized Material”) is produced by any Party in such form, the producing Party may designate such materials as Confidential by marking the container in which the media is produced “Confidential.” For electronically stored information produced in native format, designation of documents as “Confidential” may be made in a produced metadata field or in the file name. Whenever any Party receives Computerized Material or documents produced in native format that have been designated as Confidential, if such Party reduces such material to hardcopy form, that Party shall mark the hardcopy form with the “Confidential” designation.

7. If responses to interrogatories, requests for admission, or other written responses to discovery quote, summarize, or contain Confidential Material, the Parties may designate them as Confidential Material by marking the face of any such response with one of the legends set

forth in paragraph (3) above and indicating the page and line references of the material that are to be subject to this Protective Order.

8. A Party may designate the transcript of any deposition in this action or any portion thereof, including exhibits thereto, as Confidential Material by either so advising the court reporter and the Parties on the record during the taking of the deposition or within thirty (30) days after receipt of the deposition transcript by written designation served upon the Parties. If all or any portion of a deposition is designated as being subject to this Protective Order, the court reporter and any Parties possessing any transcripts shall label the cover page of each transcript or copy thereof to state that the deposition includes Confidential Material, and shall label as Confidential each of the pages of the transcript or exhibits that contain Confidential Material.

9. Any production of any confidential or proprietary material will not result in or be construed as a waiver, in whole or in part, of (a) the producing Party's claims of confidentiality either as to the specific information disclosed or more generally as to the subject matter of the information disclosed, or (b) the party's right to later designate the material as Confidential pursuant to this Protective Order. In the event that a Party produces any Confidential Material without attaching one of the legends described in paragraph (3) above, the Party may subsequently designate the material as Confidential at any time by forwarding to the opposing Party copies of the material bearing one of the legends required by paragraph (3) and requesting that the opposing Party destroy all prior copies of the Confidential Material. Upon receipt of such a request, the opposing Party shall destroy all copies of the Confidential Material as originally produced and replace them with copies bearing the appropriate confidentiality legend.

10. Written and oral communications between or among counsel for the Parties that refer to or discuss Confidential Material automatically shall be subject to this Protective Order.

11. Confidential Material shall be treated by the Parties and their counsel as being confidential and private. Any copy made of Confidential Material shall have the same status as the original. The disclosure and use of Confidential Material shall be confined to the permissible

disclosures and uses set forth below. Confidential Material shall be used (if otherwise relevant and admissible) solely for the litigation of this action, including any appeals, and for any other action brought by or on behalf of a former user of Monsanto glyphosate-containing products alleging injuries or other damages therefrom, so long as all parties are bound by and subject to another judicially approved protective and confidentiality order that is identical to or the substantial equivalent to this order and has been agreed to by Monsanto. In addition, before Confidential Material is shared with parties to other lawsuits or used for other lawsuits brought by or on behalf of a former user of Monsanto glyphosate-containing products alleging injuries or damages therefrom, the parties to the other action(s) also must have entered into an ESI protocol, protocol governing privilege logs, and protocol or agreement regarding the search and culling of data, including keyword search terms, or alternatively only to the extent that Monsanto has consented in writing. Confidential Material shall not be used for any other purpose without separate written agreement of the Party that produced the Confidential Information. All other disclosure and use of Confidential Material during the pendency of this action or after its termination are hereby prohibited. Nothing in this Protective Order, however, precludes Monsanto Company from making disclosures to government authorities to the extent that it is required to disclose Confidential Material by law.

12. Confidential Material may be disclosed only to the following persons and only insofar as it is reasonably necessary to the effective prosecution of the Parties' claims and defenses:

- a. Parties, their representatives, in-house counsel and regular employees who are actively engaged in or actively overseeing this action, or are involved in complying with any Monsanto Company legal obligations to provide information to governmental authorities;
- b. Counsel of record in this action, including their associated attorneys, paralegal and secretarial personnel, and other support staff;
- c. Experts and consultants (including their employees) who are retained by a Party to assist in this action;

- d. Third-party contractors and their employees who are retained by one or more Parties to provide litigation-support or copy services in connection with this action;
- e. Witnesses or prospective witnesses in this action;
- f. Court reporters and other persons involved in recording deposition testimony in this action;
- g. Named plaintiffs in other actions brought by or on behalf of a former user of Monsanto glyphosate-containing products alleging injuries or other damages therefrom and their counsel of record, including paralegal, clerical, secretarial and other staff employed or retained by such other plaintiffs' counsel of record if the conditions of Paragraph 11 above have been met;
- h. Court personnel of this Court, or, if on appeal, of a court with appellate jurisdiction; and
- i. Jurors in this action.

Counsel for each Party disclosing Confidential Material in accordance with this paragraph shall (i) advise each person to whom such disclosure is made (except Court personnel, jurors, and government authorities) of the terms of this Protective Order and of the obligation of each such person to comply with those terms and (ii) provide a copy of this Protective Order to each such person. Prior to the disclosure of any Confidential Information to any person identified in subparagraphs c, d, e, f and g above, such person shall sign an Acknowledgment, in the form attached hereto, acknowledging that he or she has read this Protective Order and shall abide by its terms. Counsel shall maintain a list of persons to whom confidential materials are disclosed (excluding jurors, Court personnel, and government authorities). Upon learning of any disclosure of Confidential Material to any person not authorized by this paragraph to receive Confidential Material, the Party who so learns shall immediately (i) inform in writing the Party from which the Confidential Material was originally received of such disclosure, including to whom the material was disclosed, and (ii) take all necessary steps to retrieve as soon as possible each and

every copy of all Confidential Material from the unauthorized person and any person to whom the unauthorized person disclosed the Confidential Material.

13. Disclosure of Confidential Material in accordance with this Protective Order shall not effect, nor shall it be deemed to effect a waiver of the attorney-client privilege, the work-product immunity, or any other privilege or immunity from disclosure to which such Confidential Material may be entitled, whether in this action or in any other action or as to any non-party.

14. Any use of confidential or protected material at trial shall be governed by a separate agreement or order.

15. Each Party agrees that in the event it is served by a non-party with a subpoena or request for production of Confidential Material originally received from another party, it will give sufficient notice to allow that Party a reasonable opportunity to intervene to oppose such production. The notice shall include a description of the material sought, the date and location for compliance with the subpoena or request, the identity of the requester of the Confidential Material, the docket number of the matter where requested, and all other information reasonably necessary to intervene and oppose such production.

16. CHALLENGING CONFIDENTIALITY DESIGNATIONS

16.1. Timing of Challenges. Any Party or Non-Party may challenge a designation of confidentiality at any time. Unless a prompt challenge to a Designating Party's confidentiality designation is necessary to avoid foreseeable, substantial unfairness, unnecessary economic burdens, or a significant disruption or delay of the litigation, a Party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed.

16.2. Meet and Confer. The Challenging Party shall initiate the dispute resolution process by providing written notice of each designation it is challenging and describing the basis for each challenge. No more than 500 documents shall be submitted to the challenge process in a 30-day period. To avoid ambiguity as to whether a challenge has been made, the written notice

must recite that the challenge to confidentiality is being made in accordance with this specific paragraph of the Protective Order. The parties shall attempt to resolve each challenge in good faith and must begin the process by conferring directly (in voice to voice dialogue; other forms of communication are not sufficient) within 14 days of the date of service of notice. In conferring, the Challenging Party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the circumstances, and, if no change in designation is offered, to explain the basis for the chosen designation. During the meet and confer process, the Designating Party must state the bases for its objections to each challenge on a document by document basis. A Challenging Party may proceed to the next stage of the challenge process only if it has engaged in this meet and confer process first or establishes that the Designating Party is unwilling to participate in the meet and confer process in a timely manner.

16.3. Judicial Intervention. If the Parties cannot resolve a challenge without court intervention, the Challenging Party shall file a “Notice of Improper Confidential Designation” with the Court (“Notice”). The Notice shall list the challenged documents by Bates label (or other identifying label if no Bates label). The Designating Party shall file a “Motion to Maintain Confidentiality” within fourteen (14) calendar days of the Notice, explaining why the documents should or should not be de-designated and, if applicable, why the documents are not reasonably likely to be used for any litigation purpose. Failure by the Designating Party to make such a Motion within 14 days of the Notice shall automatically waive the confidentiality designation for each challenged designation. The Challenging Party will then have seven (7) calendar days to file a Response. There shall be no Reply absent leave of Court. The Parties may stipulate in writing to allow additional time for the Designating Party to make such a Motion to Maintain Confidentiality or the Designating Party may move the Court for additional time. The burden of persuasion as to whether information is confidential shall be on the Designating Party. If the challenged documents could not reasonably be used for any litigation purpose, the Court will grant the Motion to Maintain Confidentiality without prejudice to a new objection by the

Challenging Party at a later date. Unless the Designating Party has waived the confidentiality designation by failing to file a Motion to Maintain Confidentiality as described above, all parties shall continue to afford the material in question the level of protection to which it is entitled under the Producing Party's designation until the Court rules on the challenge.

17. The production by any Party in the course of discovery in these proceedings of a document subject to a claim of privilege, work product, protection from disclosure under federal or state law, or other statutory or court-ordered confidentiality, will not result in a waiver of any of the foregoing protections, whether in these or any other proceedings, for the produced document or any other withheld document covering the same or similar subject matter. Upon notice of such disclosure, all originals and copies thereof, shall be returned to the producing Party within twenty (20) business days of receipt of such notice and the receiving party shall not use such information for any purpose until further Order of the Court. Such returned material shall be deleted from any litigation-support or other database. All notes or other work product reflecting the contents of such disclosed materials shall be destroyed, and receiving counsel shall certify in writing to the producing party's counsel compliance with this paragraph. In the event of disagreement, until such time as the disagreement is resolved, the receiving Party will return the document and will not review or use the document or its contents. If the substance of the protected document is discussed in a deposition prior to the time of discovery or notification of the inadvertent disclosure, the Parties agree that such testimony may not be used for any purpose until the dispute is resolved by agreement of the Parties or by Court order. The party to whom any produced document was returned shall retain the returned materials until the end of the case, including any appeals. Within fifteen (15) business days after notice of the disclosure, the producing Party shall provide a log that describes the basis for the claim that the material is privileged or otherwise protected from disclosure. After receipt of such a privilege log, any Party may dispute a claim of privilege or protection, however, prior to any submission to the Court for an in camera review, the Party disputing a claim of privilege or protection shall provide in writing the identification of the documents for which it questions the claim of privilege or

protection and the reasons (including legal support) for its assertion that the documents are not privileged or protected. Within fifteen (15) business days, the Party seeking to support the claim of privilege or protection shall provide a written response supporting the claim of privilege or protection (including legal support). The Parties will then meet and confer in good faith as to the claims of privilege or protection. If agreement cannot be met after ten (10) business days, any party may thereafter submit the material under seal to the Court for a determination as to privilege or protection. The burden of persuasion in any such challenge proceeding shall be on the party asserting privilege or protection.

18. The Parties will use the following procedure for submitting to the Court papers consisting of, relating to, containing, incorporating, reflecting, describing or attaching Confidential Material: consistent with the Court's Administrative Procedures for Filing Documents, any Party submitting such material shall electronically file a motion or application to file documents under seal. Documents at issue in a motion to seal will be automatically sealed unless the Court finds after 10 court days' notice to the parties with opportunity to be heard that such matter should not be sealed. Documents filed under seal do not notice out automatically from the system and must be mailed to opposing counsel. Such material shall be kept under seal until further order of the Court; however, such materials shall only be available to the Court and counsel of record, and to all persons entitled to receive such information under the terms of this Order. When serving such material, the parties shall select the "Sealed, electronic" option to ensure that online access is restricted as contemplated by this Order. The parties shall take reasonable steps to minimize such sealing. Within seven (7) days of the submission of any material under seal, the parties shall confer to determine if the Producing Party objects to the filing of the Confidential Information in unsealed form. To the extent of the parties' agreement concerning the treatment of the Protected Information, the filing party may file the subject materials in unsealed form. To the extent the parties are unable to reach agreement, either party may file a motion to address the appropriate treatment of the subject materials. On such motion, the burden of persuasion as to whether information is confidential shall be on the Designating

Party. The material shall remain sealed unless the Court orders otherwise. When exhibits to court filings are needed, the parties shall file only the pages necessary for their arguments unless the Court requests additional material.

19. This Protective Order shall not prevent the Parties from using or disclosing their own documents and other materials in any manner for any business or personal reason, notwithstanding their designation as Confidential Material subject to this Protective Order. The use or disclosure by a Party of its own documents or materials shall not terminate, waive or otherwise diminish in any way the status of such documents or materials as Confidential Materials subject to this Protective Order.

20. Upon the final determination, including any appeals related thereto, of this action, the producing Party will send a letter to the receiving Party, stating that the lawsuit has concluded and requesting that all Confidential Material be returned or destroyed. If, at that time, the producing Party has entered an agreement permitting use of the Confidential Materials in another action, the producing Party may wait until resolution of that action to send the letter. Within thirty (30) days after receipt of that letter, all attorneys in possession of Confidential Material shall return all Confidential Material to the disclosing Party or, alternatively, shall immediately destroy all such material. All counsel of record shall, within forty-five days of this final determination, certify that all Confidential Material, including any such material disclosed to any other entity, has been returned or destroyed. The sole exception to the requirements described above is that information that has been incorporated into attorney work product or other privileged documents need not be returned or destroyed. Such information shall be retained by the person to whom the information was produced, and shall be treated as Confidential Material in accordance with this Order.

21. This Protective Order shall not enlarge or affect the proper scope of discovery in this or any other lawsuit, nor shall this Protective Order imply that material designated (or not designated) as Confidential Material under the terms of this Protective Order is properly discoverable, relevant, or admissible in this or any other lawsuit.

22. Each Party shall retain all rights and remedies available to it under the law for the enforcement of this order against anyone who violates it.

23. The restrictions of this Protective Order shall continue to apply after this action is finally determined and the Court shall retain jurisdiction for all purposes in connection therewith. All persons receiving or given access to Confidential Material in accordance with the terms of this Protective Order consent to the continuing jurisdiction of the Court for the purposes of enforcing this Protective Order and remedying any violations thereof.

24. If a party concludes that certain documents require special or additional protections beyond the protections of this Order such as a designation of “Confidential – Attorneys’ Eyes Only,” the parties will meet and confer about those documents at that time and present the issue to the Court if no agreement can be reached.

IT IS SO ORDERED.

Date: _____, 2020

TERRY A. DOUGHTY
United States District Judge

EXHIBIT A
ACKNOWLEDGMENT AND AGREEMENT TO BE BOUND

I, _____ [print or type full name], of _____
_____ [print or type full address], declare under
penalty of perjury that I have read in its entirety and understand the Protective and
Confidentiality Order that was issued by the United States District Court for the Western District
of Louisiana on _____ [date] in *Berry v. Monsanto Co.*, Civil Action No. 3:20-
cv-00537-TAD-KLH . I agree to comply with and to be bound by all the terms of this Protective
and Confidentiality Order, and I understand and acknowledge that failure to so comply could
expose me to sanctions and punishment in the nature of contempt. I solemnly promise that I will
not disclose in any manner any information or item that is subject to this Protective and
Confidentiality Order to any person or entity except in strict compliance with the provisions of
this Order.

I further agree to submit to the jurisdiction of the United States District Court for the
Western District of Louisiana for the purpose of enforcing the terms of this Protective and
Confidentiality Order, even if such enforcement proceedings occur after termination of this
action.

I hereby appoint _____ [print or type full name] of
_____ [print or type full address
and telephone number] as my Louisiana agent for service of process in connection with this
action or any proceedings related to enforcement of this Stipulated Protective Order.

Date: _____

City and State where sworn and signed: _____

Printed name: _____

Signature: _____

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA**

TERRY LEE BERRY AND
NANCY BERRY,

Plaintiffs,

V.

MONSANTO COMPANY,

Defendant.

Civil Action No. 3:20-cv-00537-TAD-KLH

[PROPOSED] ORDER GOVERNING PRIVILEGE LOGS

For good cause shown, the Court hereby orders as follows:

A. **Asserting Privilege or Protection.** A party who withholds or redacts documents or information contained within a document on the grounds of attorney-client privilege and/or work product protection, or any other asserted privilege, shall provide:

1. A listing of such documents in electronic spreadsheet format providing the following objective metadata fields (“objective metadata” does not include substantive content from, or a subjective description of, the document being withheld or redacted) where available:

- a. the Bates number of the document (or unique document identifier);
- b. the nature of the privilege asserted (“attorney-client privilege” or “attorney work product”);
- c. the name(s) of the author(s) of the document (if known or knowable) (for email chains, because metadata only captures the author(s) of the most recent email in the chain, all emails in the

same chain will be listed together in the log and the emails within the chain to which privilege is asserted will state “attorney-client privilege” or “attorney work product”);

- d. the name(s) of the recipient(s) of the document, including anyone who was sent the document as a “CC” or a “BCC” (if known or knowable) (for email chains, because metadata only captures the recipients of the most recent email in the chain, all emails in the same chain will be listed together in the log and the emails within the chain to which privilege is asserted will state “attorney-client privilege” or “attorney work product”);
- e. the document type, including, for example, whether the document is an email, paper file, a spreadsheet, or other descriptive identifier of the document type; and
- f. the date the document was created (if known or knowable), sent (if applicable), and last modified (if applicable).

2. The names of the individuals who are identified prior to providing the privilege log as being attorneys will be highlighted on the log; if it is discovered that names of other attorneys on the log were not highlighted, the opposing party will be notified with an offer to provide a replacement log. In addition to the preceding paragraph, the withholding/redacting party will also include the following information in its privilege log entries (provided the party remains willing to meet and confer further on specific documents after production of this privilege log):

Document Type	From and to whom	Content
Email	from attorney to client	conveying legal advice
Email Attach.	from client to attorney	requesting legal advice
Memorandum	between attorneys	discussing legal advice
Letter	between clients	discussing litigation
Other Document	between client and attorney	prepared in anticipation of/for litigation

3. As an alternative to the categories in the preceding paragraph, or where they do not apply, the withholding/redacting party may provide alternate individualized descriptions for such documents.

B. Challenging Asserted Privilege and Protection. After receipt of such a privilege log, any Party may dispute a claim of privilege or protection, however, prior to any submission to the Court for an *in camera* review, the Party disputing a claim of privilege or protection shall provide in writing the identification of the documents for which it questions the claim of privilege or protection and the reasons (including legal support) for its assertion that the documents are not privileged or protected. Within thirty days, the Party seeking to support the claim of privilege or protection shall provide a written response supporting the claim of privilege or protection (including legal support). The Parties will then meet and confer in good faith as to the claims of privilege or protection. If agreement cannot be met after fifteen (15) business days, any party may thereafter submit the material under seal to the Court for a determination as to privilege or protection. If/when challenges are presented to the Court, the parties' positions on those documents will be affirmed by counsel pursuant to Rule 11. If a party believes the circumstances require different timing or procedure, they shall meet and confer on alternatives to resolving any disputes and if unable to agree may present the issue to the Court.

C. **Time for Providing Privilege Log.** The producing party shall provide the information required by paragraph “A” to the receiving party within 30 days of withholding or redacting the related documents.

Date: _____, 2020

TERRY A. DOUGHTY
United States District Judge

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA**

TERRY LEE BERRY AND
NANCY BERRY,

Plaintiffs,

V.

MONSANTO COMPANY,

Defendant.

Civil Action No. 3:20-cv-00537-TAD-KLH

[PROPOSED] RULE 502(D) ORDER

1. The production of privileged or work-product protected documents, electronically stored information (“ESI”) or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness, and/or segregation of privileged and/or protected information before production.

Date: _____, 2020

TERRY A. DOUGHTY
United States District Judge

II. Production Format of Defendant's Electronically Stored Information

A. Definitions

1. "Document" means paper documents or electronically stored information (ESI) existing in any medium from which information can be obtained or translated into reasonably usable form.
2. "Native File(s)" means ESI in the file type for (or of) the application in which such ESI is normally created, viewed and/or modified.
3. "Metadata" means: (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted or otherwise manipulated by a user of such system.
4. "Static Image(s)" means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. A Tagged Image File Format (TIFF) image is an example of a Static Image.
5. "Load/Unitization file" means a set of paper-scanned images or electronically processed files and indicates where individual pages or files belong together as documents, including attachments, and where each document begins and ends. A Load/Unitization file will also contain data relevant to the individual documents, such as Metadata, coded data, and OCR or Extracted Text.

6. “OCR” means the optical character recognition file which is created by software used in conjunction with a scanner that is capable of reading text-based documents and making such documents searchable using appropriate software.
7. “Extracted Text” means the text extracted from a Native File and includes all header, footer and document body information.
8. Parties will use reasonable, best efforts to comply with the terms of this production format. In the event a party determines that it cannot materially comply with any requirement herein, they will disclose their inability to comply and parties will meet and confer regarding resolution of the identified issue.

B. Format of Production

1. Paper Documents

Paper documents, including spreadsheets maintained in paper form, will be produced as TIFF images (consistent with the specifications in Section II.B.2.a.). The production will include the appropriate Load/Unitization files which will, at a minimum, contain the following fields (described in detail in Section II. B. 2. (e.) *infra.*):

- a. Beginning Production Number (ProdBeg),
- b. Ending Production Number (ProdEnd),
- c. Beginning Attachment Production Number (BegAttach),
- d. End Attachment Production Number (EndAttach),
- e. Custodian/Source,
- f. Confidentiality,

- g. Document Type,
- h. Page Counts, and
- i. OCR.TXT file.

In scanning paper documents, if a document is more than one page, to the extent reasonably possible, the unitization of the document and any attachments or affixed notes should be maintained as it existed when collected by the producing party. The parties may unitize their documents using either physical unitization (i.e., based on physical binding or organizational elements present with the original paper documents like staples, clips and binder inserts) or logical unitization (i.e., a manual review of the paper to determine what logically constitutes a document like page numbers or headers). The parties will meet and confer to resolve any related issues.

2. ESI

- a. All TIFF-formatted documents will be single page, Group 4 TIFF at 300 x 300 dpi resolution and 8.5 x 11 inch page size, except for documents that in the producing party's reasonable judgment require a different resolution or page size. The requesting party retains the right to request a TIFF image in a higher resolution or larger page size if necessary to render the image legible or understandable. If a color image is produced in black and white, the receiving party may request the producing party to produce the original, color image. After receiving such a request for color production, the parties will meet and confer on a reasonable and cost-effective means of providing the requested documents. To the extent possible, the original orientation shall be maintained (e.g.,

portrait-to-portrait and landscape-to-landscape). Such files will be grouped in folders of no more than 1,000 TIFF files each unless necessary to prevent files from splitting across a folder.

- b. In the absence of agreement of the parties or order of Court, a Static Image will be provided in TIFF format (.TIF files). The image file names shall match the Bates number assigned to the image. All documents are to be provided with multi-page searchable OCR or Extracted Text files, as described in paragraph (c).
- c. **Text Files.** Full extracted text will be provided in the format of a single *.txt file for each file (e.g., not one *.txt file per *.tif image). Where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, the redacted *.tif image will be OCR'd and file-level OCR text will be provided in lieu of extracted text. Searchable text will be produced as file-level multi-page UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the *.dat data load file.
- d. There will be two Load/Unitization files accompanying all productions. One will be the Image load file and the other will be the Metadata load file. The specifics of these files are detailed in (i) and (ii) below:

(i) **Image Load File**

- Every Document referenced in a production image load file shall have all corresponding images, text, and data logically grouped together in a directory structure with a common key to properly load the data.

- Documents shall be produced in only one image load file throughout the productions, unless that document is noted as being a replacement document in the Replacement field of the data load file.

- The name of the image load file shall mirror the name of the delivery volume, and should have an .lfp, .opt or .dii* extension (e.g., ABC001.lfp). The volume names shall be consecutive (i.e., ABC001, ABC002, et. seq.) **If .dii file is produced, the accompanying metadata load file shall be separate from the .dii file and not contained within the .dii file.*

- The load file shall contain one row per Tiff image.
- Every image in the delivery volume shall be contained in the image load file.

- The image key shall be named the same as the Bates number of the page. Load files shall not span across media (e.g., CDs, DVDs, Hard Drives, etc.), i.e., a separate volume shall be created for each piece of media delivered.

(ii) Metadata Load File

- The metadata load file shall use the following delimiters:

- Column Delimiter: Pipe – | (ASCII 124)
- Text Qualifier: Caret – ^ (ASCII 94)
- New line: Registered sign - ® (ASCII 174)
- Data for documents shall be produced in only one data load file throughout the productions, unless that document is noted as being a replacement document in the Replacement field of the data load file.
- The first record shall contain the field names in the order of the data set forth in (B. 2. e.). Metadata fields that are not applicable to a document shall be filled with a NULL value along with fields that were not able to be obtained due to a processing error or corrupt file.
- All date fields shall be produced in "mm/dd/yyyy hh:mm:ss AM" format.
- A carriage-return line-feed shall be used to indicate the start of the next record.
- Load files shall not span across media (e.g., CDs, DVDs, Hard Drives, etc.); a separate volume shall be created for each piece of media delivered.
- The name of the metadata load file shall mirror the name of the delivery volume, and shall have a .dat, .csv or .txt extension (i.e., ABC001.dat).

- The volume names shall be consecutive for each produced source. (i.e., ABC001, ABC002, et. seq.).
- e. Except as set forth herein, ESI will be produced to the requesting party as Static Images together with a Load/Unitization file that will contain the Metadata fields described below on the document level, except as set forth in section (B.) (2.) (1.) infra. The following fields associated with each electronic document including the body of the document, will be produced in the appropriate Load/Unitization file.

	Field	Summation Field (Florida)	Definition	Doc Type	Source: Load File (L) or Metadata (M)
1	SOURCE	SOURCE	Name of party producing the document	All	L
2	CUSTODIAN	CUSTODIAN	Name of person or data source (non-human) from where documents/ files are produced. <i>**Where redundant names occur, individuals should be distinguished by an initial which is kept constant throughout productions (e.g., Smith, John A. and Smith, John B.)</i>	All	M or L
3	CUSTODIAN ID	CUSTODIAN ID	Each CUSTODIAN from #2 above will be assigned a unique numeric identifier that will be maintained throughout productions.	All	M or L
4	BEGBATES	BEGDOC#	Beginning Bates Number (production number)	All	L
5	ENDBATES	ENDDOC#	End Bates Number (production number)	All	L
6	PGCOUNT	PGCOUNT	Number of pages in the document	All	L
7	FILESIZE	FILESIZE	File Size	All	M

	Field	Summation Field (Florida)	Definition	Doc Type	Source: Load File (L) or Metadata (M)
8	APPLICAT	APPLICAT	Commonly associated application for the specified file type. (See 2 (l) below).	All	M
9	FILEPATH	FILEPATH (for Edocs) FOLDER (for emails)	File source path for all electronically collected documents and emails, which includes location, folder name, file name, and file source extension.	All	M
10	NATIVEFILELINK	DOCLINK	For documents provided in native format only	All	L
11	TEXTPATH	LOGFILE or FULLTEXT	File path for OCR or Extracted Text files per paragraph (d) above	All	L
12	MSGID	MSGID	Email system identifier assigned by the host email system. Value extracted from parent message during processing	Email	M
13	FROM	FROM	Sender	Email	M
14	TO	TO	Recipient	Email	M
15	CC	CC	Additional Recipients	Email	M
16	BCC	BCC	Blind Additional Recipients	Email	M
17	SUBJECT	SUBJECT	Subject line of email	Email	M
18	PARENTBATES	PARENTID	BeginBates number for the parent email of a family (will not be populated for documents that are not part of a family)	Email	L
19	ATTACHBATES	ATTACHID	Bates number from the first page of each attachment	Email	L
20	BEGATTACH	(will be provided from ATTRANGE)	First Bates number of family range (i.e. Bates number of the first page of the parent email)	Email	L
21	ENDATTACH	(will be provided from ATTRANGE)	Last Bates number of family range (i.e., Bates number of the last page of the last attachment)	Email	L
22	ATTACHCOUNT	ATTACHMENT COUNT	Number of attachments to an email	Email	L
23	ATTACHNAME	ATTACHMENT LIST	Name of each individual attachment	Email	M

	Field	Summation Field (Florida)	Definition	Doc Type	Source: Load File (L) or Metadata (M)
24	DATESENT (mm/dd/yyyy hh:mm:ss AM)	DATESENT	Date Sent	Email	M
25	DATERCVD (mm/dd/yyyy hh:mm:ss AM)	DATERCVD	Date Received	Email	M
26	EMAILDATSORT (mm/dd/yyyy hh:mm:ss AM)	DATESENT	Sent Date of the parent email (physically top email in a chain, i.e. immediate/direct parent email)	Email	L
27	READ/UNREAD		Whether the Outlook item was read or unread at the time of collection. Values provided will be "Yes" for read, "No" for unread, and a null value where the read/unread flag value is unavailable.	Email	M
28	Email Outlook Type	Email Outlook Type	Type of Outlook item, e.g. email, calendar item, contact, note, task	Email	M
29	HASHVALUE	MD5 HASH	MD5 Hash Value for Edocs	Edocs	M
30	TITLE	DOCTITLE	Title provided by user within the document	Edocs	M
31	AUTHOR	AUTHOR	Creator of a document	Edocs	M
32	DATECRTD (mm/dd/yyyy hh:mm:ss AM)	DATECRTD	Creation Date	Edocs	M
33	MODIFIED BY	LAST EDITED BY	Person who has modified a document	Edocs	M
34	LASTMODD (mm/dd/yyyy hh:mm:ss AM)	LASTMODD (mm/dd/yyyy hh:mm:ss AM)	Last Modified Date	Edocs	M
35	DocumentType	DocumentType	Descriptor for the type of document: "E-document" for electronic documents not attached to emails; "Emails" for all emails; "E-attachments" for files that were attachments to emails; and "Physicals" for hard copy physical documents that have been scanned and converted to an electronic image.	All	M

	Field	Summation Field (Florida)	Definition	Doc Type	Source: Load File (L) or Metadata (M)
36	Importance	Importance	High Importance – indicates Priority in Email message.	Email	M
37	Redacted	Redacted	Descriptor for documents that have been redacted. "Yes" for redacted documents; "No" for unredacted documents.	All	M
38	ProdVol	ProdVol	Name of media that data was produced on. Wave 001 – Hard Drive	All	M
39	Confidentiality	Confidentiality	Indicates if the document has been designated as “Confidential” pursuant to any applicable Protective Order. “Yes” for Confidential documents; “No” for documents that are not so designated.	All	M
40	Color	Color	Flag to indicate that document contains color. Values provided will be “Yes” for color, “No” for no color,	All	M
41	FILENAME	@C FILENAME	Original filename at the point of collection, without extension of native file	All	M
42	FILEEXTENSION	@C FILEEXT	File extension of native file	All	M

This list of fields does not create any obligation to create or manually code fields that are not automatically generated by the processing of the ESI; that do not exist as part of the original Metadata of the document; or that would be burdensome or costly to obtain. The parties retain the right to move the Court for the production of additional electronic metadata fields should ongoing discovery reveal the need for such Metadata. The designation of a document as a "Protected Document" pursuant to the Protective Order of Confidentiality shall include the metadata produced for that document.

- f. **Bates Numbering:** All images must be assigned a Bates/control number that shall always: (1) be unique across the entire document production, (2) maintain a constant length (zero/0-padded) across the entire production, (3) contain no special characters or embedded spaces, and (4) be sequential within a given document. If a Bates number or set of Bates numbers is skipped in a production, and not otherwise identified on a privilege log, the producing party will disclose the Bates numbers or ranges in a cover letter accompanying the production. Production Bates numbers shall be endorsed on the lower right corner and shall not obscure any portion of the original file. Confidentiality designations, if any, shall be endorsed on the lower left corner of applicable images and shall not obscure any portion of the original file.
- g. When processing ESI, **GMT** should be selected as the time zone. To the extent that a party has already processed ESI using a different time zone, the producing party will note the time zone used in its processing.
- h. Documents with dynamic fields for file names, dates, and times will be processed to show the field code (*e.g.*, “[FILENAME]” or “[AUTODATE]”), rather than the values for such fields existing at the time the file is processed.

- i. When the Static Image is produced, the producing party shall make reasonable attempts to maintain and not modify the original Native File and its metadata.
- j. The parties will meet and confer regarding collection and production of ESI stored in databases and other structured data under the custody and control of the parties.
- k. Electronic file collection will be “De-NISTed”, removing commercially available operating system and application files contained on the current NIST file list. Identification of NIST list matches will be through MD5 Hash values.
- l. User-generated files that have been collected that cannot be produced and/or imaged because of technical issues should be identified as exception files and included on a log that lists all metadata set forth in paragraph 2(e) except that the metadata for the APPLICAT field will be obtained from binary encoding from the file, and reason for exception: for example, corruption, unavailable password protection, proprietary software, or other technical issues. The producing party shall provide a copy of this log with its production. If the receiving party requests production of any files listed on the exception log, the parties will meet and confer, including on any reasonable and cost-effective means of providing the requested data.

m. “Duplicate ESI” means files that are exact duplicates based on the files’ MD5 or SHA-1 hash value. The producing party need only produce a single copy of responsive Duplicate ESI. De-duplication shall not break apart families and shall be performed at a family level. Defendants will globally (e.g., both within a particular custodian’s file and across all custodian/databases) de-duplicate identical ESI as follows:

- (1) Electronic Files: Electronic files will be de-duplicated based upon calculated MD5 Hash values for binary file content. File contents only will be used for MD5 Hash value calculation and will not include operating system metadata (filename, file dates) values.
- (2) Messaging Files: Messaging files will be de-duplicated based upon MD5 Hash values for the message family, including parent object and attachments. The following fields will be used to create the unique value for each message: To; From; CC; BCC; Date Sent; Subject; Body; and, MD5 Hash values for all attachments, in attachment order. Messaging materials will be de-duplicated at a family level, including message and attachment(s).
- (3) Log Files: For the existing file collection containing fully processed duplicate files and messages, duplicate documents will be listed in a de-duplication log including the same agreed

production format meta-data structure and data delivery criteria as for the "master" production documents. Moving forward, as collected electronic materials are globally de-duplicated during system intake using the above guidelines, defendants will produce logs containing the meta-data field values for de-duplicated files. As document production begins for additional custodians and during rolling productions for existing custodians, an updated de-duplication log shall be produced for each production. The metadata provided will be an accurate representation of the data existing for the documents at the time of collection.

- n. **Parent-Child Relationship.** Parent-child relationships (e.g., the associations between emails and their attachments) shall be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent or email or ESI records. Parent-child relationships will be identified in the data load file pursuant to paragraph II. B. 2. e.
- o. **Email Threading.** Email threads are email communications that contain prior or lesser-included email communications that may also exist separately in a Party's electronic files. A most inclusive email thread is one that contains all of the prior or lesser-included e-mails, including attachments, for that branch of the email thread. The Producing Party shall produce the most inclusive email thread and

all prior or lesser included email threads that were collected and identified as responsive and not privileged.

- p. **Embedded Objects:** Objects embedded in Microsoft Word and .RTF will be extracted as separate documents and produced as attachments to the document.
- q. **Compressed files.** Compression file types (i.e., .CAB, .GZ, .TAR, .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual folders and/or files.
- r. **Replacement files:** Any documents that are replaced in later productions shall be clearly designated as such, by appending a “-R” to the production prefix and by a letter accompanying the production clearly designating such documents as replacements.
- s. **Native Files.** The parties acknowledge that production in TIFF and load file format may be inadequate for certain types of ESI (e.g. spreadsheets). The following files shall be produced in native format (except for redacted documents):
 - i. All audio files and video files shall be produced in native format with the source file path provided.
 - ii. Electronic spreadsheet (e.g., Excel), electronic presentations (e.g., PowerPoint), desktop databases (e.g., Access), and audio/video multimedia files shall be produced in native format whenever possible. The production of the electronic

spreadsheets shall include hidden rows, columns and worksheets. Native Excel files will be redacted by overwriting the data contained in a particular cell, row, column or tab with the term “REDACTED.” If the production party deems it necessary to produce redacted Excel (or other spreadsheet formats) in any format other than Native, the parties should meet and confer before such a production is made.

- iii. Electronic presentations (e.g. PowerPoint). The production of the electronic presentation files shall include comments, hidden slides, speaker notes, notes and similar data. To the extent native files are produced without an accompanying rendering of TIFF images, a slip sheet will be produced in TIFF format to facilitate Bates and confidentiality stamping. If documents requested in native format require redactions, the parties will produce TIFF images for those documents. Confidentiality of documents produced in native will be noted in the File Name along with the Bates number and in a metadata field. If a dispute arises with respect to the provision, the parties agree to meet and confer in an effort to resolve their differences. Should the producing party collect Statistical Analysis System, the parties shall meet and confer regarding production format prior to production.

- iv. **Word Processing Files.** Word processing files including limitation Microsoft Word files (*.doc and *.docx), with tracked changes and comments showing. Such word files will be produced in native format.
- t. **Emails:** Emails will be produced with the CC and BCC line displayed.
- u. **Word Processing Files.** Word processing files, including without limitation Microsoft Word files (*.doc and *.docx), will be produced with tracked changes and comments showing. Supplemental requests for native format and color copies will be governed by Section II. B. 2. a, above.
- v. Any native files that are produced shall be produced with the source file path provided, as well as all extracted text and applicable metadata fields set forth in Section II. B. 2. e.
- w. The parties shall exchange production samples as follows: (1) standard production from each source (physical, email, electronic document, native, etc.) which fully exercises the metadata fields set forth above; (2) replacement production; (3) clawback.
- x. **Redacted Document Log.** The producing party will provide a log identifying by bates/production number each document that contains a redaction and the reason for the redaction. In addition, if the redaction is based on attorney-client privilege or the work-product doctrine, the document also will be addressed on the

privilege log and comply with any order entered governing the privilege log.

- y. **Privilege Log.** Privilege logs shall be produced in PDF format, and shall be accompanied by an Excel copy of the log. The PDF copy will be the official privilege log of record. The privilege log also shall comply with any order entered governing the privilege log.
- z. **Suppressed Metadata Log.** The producing party will provide a log identifying by bates/production number each document that contains metadata field values subject to Privacy or Privilege exceptions. Suppressed field values will be replaced in whole with a “REDACTED” placeholder value. The log will provide the document BEGBATES value, field name suppressed and the suppression reason.
- aa. **Foreign Language Documents.** All documents shall be produced in their original language. If two documents are substantially identical except that they are in different languages, they shall not be treated as exact duplicates. Nothing in this agreement shall require a producing party to prepare a translation or certify the translation that they possess.

C. Objections to Production of ESI

- 1. Nothing in this agreement waives a party’s right to object to production of ESI that is not reasonably accessible because of undue burden or cost. The identification of documents pursuant to this ESI Protocol need not include

searches of ESI from sources that are not reasonably accessible because of undue burden or cost. Such sources that are not reasonably accessible include, but are not limited to: (a) deleted, fragmented or slack data; (b) random access, cache or other ephemeral data; (c) ESI contained on “Backup Systems” (*e.g.*, systems that periodically store electronic information on tape or comparable media to permit recovery of the information in the event of a system failure); (d) on-line data access data such as temporary internet files or cookies; and (e) ESI that cannot be directly opened by its native application due to conversion to a different format for backup or archival purposes.

2. If asserting an objection based on paragraph II(C)(1), the responding party will inform the requesting party of the electronic information it is willing to produce, the nature and location of the information claimed to not be reasonably accessible, the reason(s) why the requested production would impose an undue burden or is unreasonably costly, and afford the requesting party an opportunity to propose an alternative means of compliance with the request, including payment of all or part of the costs of retrieving the information. If an agreement cannot be reached as to the producing party’s objection to production, the parties shall seek judicial assistance.

D. Continuing Obligations

1. To expedite discovery of relevant electronic evidence and reduce costs, the parties’ computer experts will informally cooperate and discuss procedures or protocols to facilitate identification, retrieval and production of

computerized information. This responsibility shall be continuing, unless otherwise ordered by the Court.

2. The inadvertent production of any materials constituting or containing attorney-client privileged information or attorney work product shall not waive any claim of privilege. If a receiving party disclosed the document(s) or information contained in the document(s) before being notified of its inadvertent production, the receiving party shall take reasonable steps to retrieve that information until the privilege claim has been resolved.
3. The parties will work with one another in good faith to resolve any issues, disputes or objections that arise in connection with electronic discovery issues before raising such matters with the court. Issues shall be raised promptly in writing, and the parties shall have good faith discussions to attempt to resolve the matter. The parties will use their best efforts to raise any objections or other requests related to a production within ninety (90) days of receipt of that production. In any event, the parties must raise any objections or other issues sufficiently in advance of the close of discovery to permit good faith negotiations to resolve the matter and briefing of any related motion such that the court has a reasonable time to rule thereon prior to the close of discovery.

III. Encryption. To maximize the security of information in transit, any media on which documents are produced may be encrypted by the producing Party. In such cases, the producing Party shall transmit the encryption key or password to the requesting Party, under separate cover, contemporaneously with sending the encrypted media.

- IV. Other Agreements.** Other orders have been proposed to the Court, may have already been entered, or will be entered in the future that supplement, complement, or otherwise impact application of this Order and/or discovery in this case. For example, the parties note that this Order does not govern the content of privilege logs except as noted and a protective and confidentiality order is contemplated. This Order also does not address the scope of discovery, timing and order of discovery, and the procedure for search and culling of documents to be reviewed.
- V. Reservation.** Each party reserves the right to object to production of documents in the format described herein to the extent that production in such format is impracticable or unreasonably burdensome or expensive.

Date: _____, 2020

TERRY A. DOUGHTY
United States District Judge